Report

Ensuring U.S. Air Force Operations During Cyber Attacks Against Combat Support Systems

Guidance for Where to Focus Mitigation Efforts

Don Snyder, George E. Hart, Kristin F. Lynch, John G. Drew

RAND CORPORATION

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2015		**00-00-2015 to 00-00-2015**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Ensuring U.S. Air Force Operations During Cyber Attacks Against Combat Support Systems: Guidance for Where to Focus Mitigation Efforts	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Rand Corporation,Project Air Force,1776 Main Street, P.O. Box 2138,Santa Monica,CA,90407-2138**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**37**	

For more information on this publication, visit www.rand.org/t/RR620

Library of Congress Cataloging-in-Publication Data is available for this publication.

ISBN: 978-0-8330-8629-7

Published by the RAND Corporation, Santa Monica, Calif.

Preface

The threats to cyberspace are increasing. The U.S. Air Force must be prepared to sustain operations in the face of attacks through cyberspace by state and nonstate actors, including attacks on its combat support. Combat support functions can be attacked by cyber means in various ways—on networks, hardware, and databases. Even though cyber defense responsibilities do not fall within the direct responsibilities of the combat support community, the obligation to carry on combat support missions (and enable the operational missions they support) does rest directly on the combat support communities, including when the attacks come through cyberspace.

Assessing the risks of losing some combat support functions because of cyber attacks is challenging because there are so many potentially vulnerable information systems that support a very large number of combat support functions and processes. Given this large number of potential targets for attack and the wide range of combat support functions and processes, where should efforts be applied for the best mitigation? The work presented in this report describes an approach to prioritize mitigation of cyber attacks against combat support information systems, and by doing so, aids in planning for more resilient Air Force operations in the event of a cyber attack on its information systems.

The work was intended to be executed in two parts: the first addressing how to focus attention on the most critical information systems and combat support functions, and the second to address in detail how to mitigate the effects of a cyber attack on these most critical information systems and functions. The activation of the budget sequestration mechanism of the Budget Control Act of 2011 (Public Law 112-25) prevented the full scope of the project from being executed, and the intended investigation of mitigation strategies was curtailed.

This research was completed as part of the project "Fighting Through a Logistics Cyber Attack." The work was conducted within the Resource Management Program of RAND Project AIR FORCE and was commissioned by the U.S. Air Force Materiel Command. It should be of interest to support, operations, and cyber communities within the U.S. Air Force.

RAND Project AIR FORCE

RAND Project AIR FORCE (PAF), a division of the RAND Corporation, is the U.S. Air Force's federally funded research and development center for studies and analyses. PAF provides the Air Force with independent analyses of policy alternatives affecting the development, employment, combat readiness, and support of current and future air, space, and cyber forces. Research is conducted in four programs: Force Modernization and Employment;

Manpower, Personnel, and Training; Resource Management; and Strategy and Doctrine. The research reported here was prepared under contract FA7014-06-C-0001.

Additional information about PAF is available on our website:
http://www.rand.org/paf/

Contents

Summary

While combat support communities are not responsible for defending cyber networks, they are required to ensure mission execution, including when under cyber attack. Assessing mission assurance for combat support when under a cyber attack is challenging. The fact that many combat support systems do not reside on the most secure networks indicates potential vulnerabilities to cyber attack. Yet the sheer number of information systems that can be attacked, the range of vulnerabilities that these might have, the large number of combat support functions they support, and the complicated connections all of these have to operational missions makes assessments difficult. Add to this the evolving nature of the threats and vulnerabilities in cyberspace, and the task of finding adequate mitigation plans for all possibilities is formidable.

What is needed is a way to pare down the problem that highlights the combat support functions and information systems of highest concern in order to focus resources on developing adequate mitigation plans for these. This report presents a sequential process for identifying those functions and information systems most likely to be problematic for the operational mission during cyber attacks. The method is implemented in a Microsoft Excel-hosted decision support tool that does not require any special expertise in the cyber domain.

The approach finds the functions and information systems that are simultaneously the most critical to the mission—defined as those that cause repercussions to the operational mission the fastest and those that have the highest risk of attack as defined by the threat, their vulnerability, and the impact of an attack. These assessments are conditional on contingency and potential adversaries. The results place the most critical functions and information systems toward the top of the rankings and the least critical toward the bottom, but given the use of proxies in the assessments, there will be some inaccuracies in detail. We recommend that the results be used as triage to determine a range of functions and information systems for further scrutiny. Using a sequential approach to these assessments, the seemingly intractable problem of assessing countless information systems, threats, vulnerabilities, combat support functions, and potential repercussions to the mission becomes manageable, and indicates areas of most benefit for more detailed assessment of mitigation strategies.

Acknowledgments

We thank Brigadier General Theron G. (Glenn) Davis, who commissioned this work, for his support throughout. We received help and feedback from too many people in the Air Force to acknowledge them all, but we would especially like to thank Lorna Estep, Shawn Lyman, Colonel Randall Gilhart, and Richard Moore in Air Force Materiel Command for their assistance and comments at various stages in the project.

At RAND, Jim Powers gave generously of his time and expertise in helping us make the decision support tool efficiently coded and robust for the user; he also reviewed an earlier draft of this report. We also thank Mahyar Amouzegar, Elizabeth Bodine-Baron, Dan Romano, Anthony Rosello, and Lara Schmidt for discussions and feedback. Cynthia Dion-Schwarz and Myron Hura provided reviews that strengthened this final report.

That we received help and insights from those acknowledged above should not be taken to imply that they concur with the views expressed in this report. We alone are responsible for the content, including any errors or oversights.

Abbreviations

ABE	AFMC Business Environment
AFMC	Air Force Materiel Command
C-NAF	Component Numbered Air Force
DCAPES	Deliberate and Crisis Action Planning and Execution Segments
IT	information technology
LCRIT	Logistics Cyber Risk Identification Tool
NIPRNet	Nonsecure Internet Protocol Router Network
OODA	observe, orient, decide, and act
PAF	Project AIR FORCE
PKI	public key infrastructure
SCADA	Supervisory Control and Data Acquisition

1. Analyzing Cyber Attacks Against Combat Support

Introduction

It is an axiom of military operations that no plan survives first contact with the enemy. Regardless of how well things are planned and how well prepared forces might be, things go awry during war and forces must be able to adapt. Circumstances that drive the need to adapt come in many forms ranging from environmental factors, such as inclement weather, to deliberate attacks from the enemy, such as theater ballistic missile and special operations attacks. For mission assurance, all airmen, whether they provide support functions or directly execute operations, need countermeasures that enable them to carry out their missions in spite of such impediments.

One relatively new class of impediments arises from the increasing use of cyberspace in nearly all functions and processes in the Air Force, including combat support.[1] Many functions and processes use—or, to some extent, depend on—cyberspace to perform their assigned missions. Scores of information technology (IT) systems have been introduced to make operations more efficient, and countless industrial control systems use network-connected Supervisory Control and Data Acquisition (SCADA) systems to govern critical utilities such as water, electrical power, and fuel. Many of these information systems lie outside U.S. Air Force control because they were made by foreign firms or are under the management of commercial firms or foreign entities.[2] As all of these systems reside in cyberspace, they are potentially vulnerable to some form of malicious adversary cyberspace operations.[3] Even though the combat support communities are not directly responsible for cyber defense,[4] they are responsible for

---

[1] By *cyberspace*, we mean "a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers." U.S. Department of Defense (DoD), *Department of Defense Dictionary of Military and Associated Terms*, Washington, D.C.: Joint Chiefs of Staff, Joint Publication (JP) 1-02, November 8, 2010 (as amended through November 15, 2013). *Combat support* is "the foundational and crosscutting capability to field, base, protect, support, and sustain Air Force forces across the range of military operations." U.S. Air Force, *Combat Support*, Washington, D.C.: United States Air Force, Air Force Doctrine Document (AFDD) 4-0, April 23, 2013.

[2] We will use the term *information system* in this report to refer to anything that might be attacked through cyberspace, including IT systems and SCADA systems. The definition conforms to that found in Committee on National Security Systems, *National Information Assurance (IA) Glossary*, CNSS Instruction No. 4009, Washington, D.C., April 26, 2010.

[3] By *cyberspace operations*, we mean "the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace" (DoD, 2010). The term is broad enough to embrace both deliberate attacks and intelligence collection.

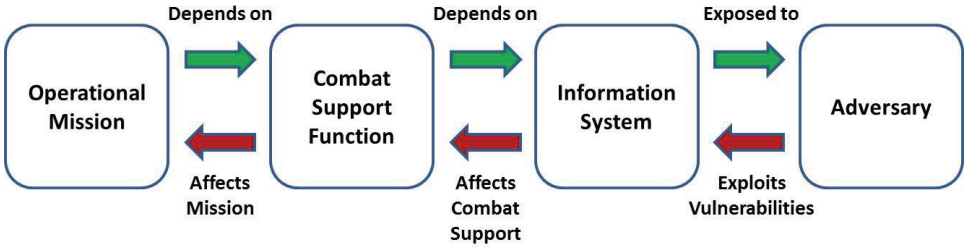
[4] U.S. Air Force, *Cyberspace Operations*, Washington, D.C.: Department of the Air Force, Air Force Policy Directive 10-17, July 31, 2012.

ensuring that they can carry out their support functions while under attack and have responsibilities for some information systems as authorizing officials.[5]

Debate continues about how worrisome malicious cyberspace operations might be. One side of the debate warns of potential future catastrophic cyber attacks that might paralyze the nation.[6] The other side sees cyber attacks as indecisive in military operations.[7] The true impact of a particular cyber attack on an Air Force mission depends on a range of details, including the vulnerability of supporting information systems, the role those information systems play in the mission, and the availability of countermeasures. In this report, we focus on potential cyber attacks against combat support information systems.

When an adversary attacks an information system, the effects can cascade, as shown in simplified form in Figure 1.1. Reading from right to left in the figure, an adversary's attack through cyberspace will cause certain effects on an information system. Those effects will have ramifications on the ability to carry out one or more combat support functions, and the effects on combat support functions will, in turn, have repercussions on the ability to carry out operational missions.

Figure 1.1. Schematic Depiction of Cascading Effects of a Cyber Attack



Assessing the dangers posed to Air Force operational missions by malicious cyber operations that target combat support functions is hampered by several factors. One is the scale and complexity of the possible paths in which an attack can affect an operational mission. The complexity of the paths works both directions in Figure 1.1. For example, consider an operational mission of air superiority that requires generating F-15C aircraft at a deployed location. The ability to carry out that mission could be endangered by failure of any one of roughly a dozen different combat support functions needed to generate F-15Cs. One of those support functions is maintenance, which is supported by 21 different information systems

[5] DoD, *Cybersecurity*, Instruction 8500.01, Washington, D.C.: DoD Chief Information Officer, 14 March 2014.

[6] For example, Richard A. Clarke and Robert Knake, *Cyber War: The Next Threat to National Security and What to Do About It*, New York: HarperCollins, 2010.

[7] For example, Martin C. Libicki, *Cyberdeterrence and Cyberwar*, Santa Monica, Calif.: RAND Corporation, MG-877-AF, 2009.

identified in the Component Numbered Air Force (C-NAF) Architecture.[8] The other support functions also depend on multiple information systems, any of which might be attacked through cyberspace. Further, a given attack could have any one (or more) of many different effects on any information system attacked. The risk to just this one aspect of a mission—generating deployed F-15Cs for air superiority—is challenging to trace through to all of the possible attacks.

Approaching Figure 1.1 from the right-hand side, consider the consequences of a cyber attack on a single information system; for example, the Deliberate and Crisis Action Planning and Execution Segments (DCAPES) system. DCAPES is the Air Force system to present, plan, source, mobilize, deploy, account for, sustain, redeploy, and reconstitute deployment requirements. At least 13 combat support functions and subfunctions need this system as a critical component of their operations. Depending on exactly how DCAPES might be affected by a cyber attack, the repercussions for each of these combat support functions are likely to be different, and there are few if any operational missions that do not require at least one of these combat support functions. Some combat support missions can also be considered operational missions in their own right (e.g., explosive ordnance disposal). To compound the complexity, the cascading ramifications will depend on the scenario of interest. Even when the lines connecting information systems to operational missions are few and clear, it is still difficult to trace all these operational repercussions.[9]

These complications not only challenge analysis, but also render it difficult to mitigate all possible attacks, leaving Air Force leaders with the conundrum of prioritizing mitigation efforts. This report tackles that challenge by describing a method to systematically rank the impacts of cyber attacks to combat support, thus indicating where efforts for mitigation are best focused.

The approach we take is built on a paramount assumption—that in the event of a cyber attack, the goal of the Air Force is to achieve operational *mission* assurance rather than *information* assurance. That is to say, the goal is to ensure that the operational missions can be executed to the maximal extent possible in the event of the most damaging cyber attack to combat support systems. Referring to Figure 1.1, information assurance focuses on continuity of operations of the information system box; mission assurance focuses on the continuity of the operational mission box.

The goal of mission assurance is less demanding than information assurance, which requires protection of all information systems and assurance that information remains accurate and available at all times. No failure is tolerable. The perspective of mission assurance is one of ensuring that the mission succeeds even though some supporting elements of the mission might fail. Mission assurance requires that the full system of information systems, combat support

---

[8] Secretary of the Air Force, Warfighting Integration and Chief Information Office, "Component NAF 2008 Architecture: Federated AFFOR/AOC Architecture," Version 2.1, 14 January 2008, distribution authorized to DoD and U.S. defense contractors only.

[9] For example, see Scott Musman, Aaron Temin, Mike Tanner, Richard Fox, and Brian Pridemore, "Evaluating the Impact of Cyber Attacks on Missions, *M&S Journal*, Vol. 8, No. 2, Summer 2013, pp. 25–35.

functions, and operational missions shown in Figure 1.1 be robust against adversary attacks. A robust system can have components that fail. The mission assurance perspective leads us to identify which components cause the system to fail gracefully, which cause the system to fail catastrophically, and which are in between. In this sense, the problem is more tractable than information assurance and keeps the focus on the desired outcome.

Our approach also acknowledges that the cyberspace domain is changing rapidly. Given the evolving nature of information systems, vulnerabilities, and threats through cyberspace, any analysis of attack impacts and mitigations must be adaptive. Therefore, the methodology described in this report, and the associated implementation of the methodology in the form of a decision support tool, is designed to be operated by Air Force personnel with limited subject matter expertise, and can be used and updated as frequently as deemed necessary to keep an adversary outside the Air Force's observe, orient, decide, and act (OODA) loop.[10]

Approach

Publicly revealed malicious cyberspace operations in the past several years demonstrate a range of damage, from denial of service up to destruction or alteration of data and physical effects on the operations of systems.[11] Many of the information systems that support combat support functions reside on the Nonsecure Internet Protocol Router Network (NIPRNet) or on networks of commercial firms, making them potentially more vulnerable to cyber attacks than information systems residing on more highly protected networks. How vulnerable are combat support functions to cyber attacks, how might such attacks affect operations, and how might those impacts be mitigated?

Analyzing these issues with a brute force approach is impractical because of the sheer number of permutations to assess and the constantly evolving nature of the information systems, vulnerabilities, and threats. The Air Force counts 25 combat support functional communities, many of which have numerous subfunctions, and the sum of the functions are supported by hundreds of information systems.[12] In addition to the number of potentially vulnerable information systems, there are also numerous ways in which a cyber attack can occur and a variety of impacts that might result. These include denial-of-service attacks from outside a firewall, manipulating data (adding, modifying, or deleting) from within a firewall, interrupting

[10] The concept of an OODA loop was put forward by John Boyd. The central idea is that in a conflict between two adversaries, if one side can observe, orient, decide, and act faster than the other, it gains the initiative and keeps the adversary confused. Boyd never formally published his work; for a discussion, see Lawrence Freedman, *Strategy: A History*, New York: Oxford University Press, 2013, pp. 196–201.

[11] See, for example: Verizon RISK Team, *2013 Data Breach Investigations Report*, Verizon, 2013; David Albright, Paul Brannan, and Christina Walrond, *Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?* Washington, D.C.: Institute for Science and International Security, December 22, 2010; and Nicolas Falliere, Liam O. Murchu, and Eric Chien, *W32.Stuxnet Dossier*, Version 1.4, Symantec Security Response, February 2011.

[12] U.S. Air Force, 2013.

communications, taking control of a SCADA system, and others. Analyzing every possible attack on all systems and assessing the impact to both combat support and operations would be impractical. Even if it were done, the results from such an analysis would be obsolete before it was finished.

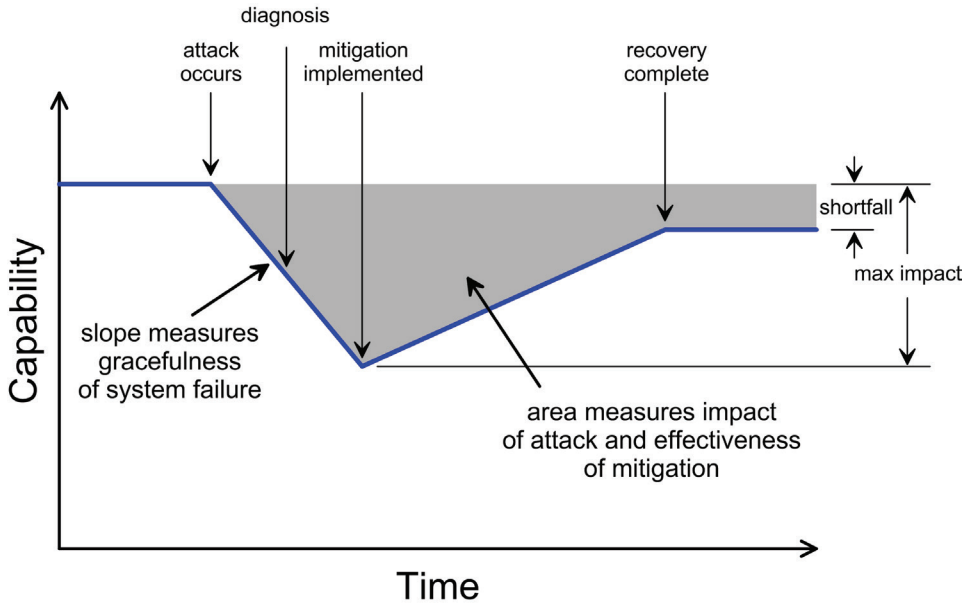
A clear need exists for prioritizing mitigation efforts. But how can we identify the most critical combat support functions and process for mitigation when, in general, the complete span of combat support is needed to carry out operational missions? An answer lies in the goal of ensuring *operational* continuity of essential missions. The objective of mission assurance leads us to seek resiliency for Air Force operations, by which we mean the ability to maintain essential operational missions during cyber attacks, and for operations to degrade gracefully when they are negatively affected.[13] The graceful-degradation-under-attack characteristic of resilient systems leads us to focus on two aspects of the aftermath of an attack: (1) the time elapsed between when combat support is negatively affected and when mission execution is negatively affected, and (2) the effectiveness of any mitigation implemented after the attack, measured by how quickly and how fully the mitigation restores operations.

The Impact of an Attack

These two aspects of the aftermath of an attack can be seen in fuller context in Figure 1.2, which shows key elements of an attack and associated response. The line on the plot indicates a certain level of capability to perform an operational mission over time. When an attack occurs, the associated combat support function is negatively affected, and then the operational capability begins to degrade. If the effects to operations are immediate, the slope will be vertical and the system degrades catastrophically. If the effects are gradual, the slope is shallow, and the system degrades gracefully. This slope is determined by the nature of the system's function. Recovery depends on how long it takes to diagnose the problem (what is the cause—is it a cyber attack?) and how long it takes to implement a mitigating solution. The mitigation will restore the capability over time, perhaps to the original level, perhaps to a reduced level. The overall impact of the attack can be measured by either the point on the line indicating maximum loss of capability or by the shaded area in the figure that incorporates the factor of time. It might be the case that recovery of the information system never occurs, but mitigations should be available to restore combat support functions, and therefore operational missions.

[13] Definition adapted from Brad Allenby and Jonathan Fink, "Toward Inherently Secure and Resilient Societies," *Science*, Vol. 309, 2005, p. 1034.

Figure 1.2. Generalization of the Failure and Recovery of a Capability After an Attack



In summary, the two largest factors that determine the impact of an attack are (1) how gracefully some capability to perform operational missions degrades as a result of the attack, and (2) the effectiveness of the mitigation used as a countermeasure, generally a course of action implemented from a continuity of operations plan.

After an Attack: How Gracefully Operations Degrade

Given the focus on mission assurance, the key measure we define for the criticality of some combat support function or process is how quickly the operational mission would be affected if the combat support function or process vanished. This timescale is a direct measure of how gracefully operations degrade from the loss of combat support. In some cases, such as the loss of aviation fuel delivery, the impact would be within hours, if not faster. For the loss of a pipeline of spare parts, the effects might take weeks if adequate readiness spares packages are available. For the loss of wind tunnel functionality at a test facility, it might take years for an operational mission to feel an impact.

After an Attack: Effectiveness of Mitigation

Mitigations can take two forms—those put in place prior to an attack, and those implemented after an attack has occurred and been properly diagnosed. These two forms are sometimes sides of the same coin. To have an adequate mitigation available to implement after an attack, certain preparations must often be done prior to the attack.

In order to have the most effective options available for mitigation, it is important not to restrict mitigations of a cyber attack to defending cyber systems alone. Cyber mitigation is not

the sole responsibility of the communications and cyber organizations in the Air Force. Mission assurance is everyone's responsibility—and many, perhaps most, mitigations will take forms other than cyber defense.

Given the goal of mission assurance (rather than information assurance), a broad palette of mitigations should be examined. For example, to mitigate against an effective cyber attack against the Standard Base Supply System, one or both of the following actions might be considered: improve the protection of the information system (e.g., move the system to a more secure network), or make the supply information system more robust to the loss of information from the field (e.g., be able to transition from a "pull" system to a "push" system when information is cut off from deployed units). Actions would need to be put in place for either of these mitigations prior to the attack to enable them to work, including development of concepts of operations, making any needed changes to systems, and training.

Methodology

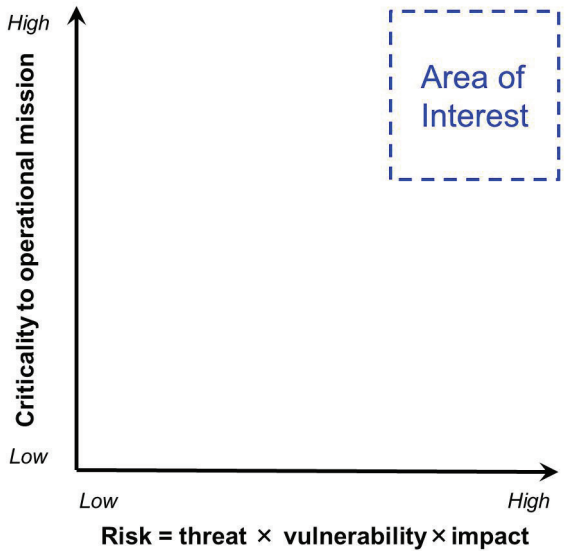
The guiding principle for our methodology is that of operational mission assurance after a cyber attack, together with the major constraints of being able to (1) pare down to an actionable number the information systems and functions that are most in need of sound mitigation strategies, given the vast number of information systems, vulnerabilities, and threats to address; and (2) do such analysis rapidly and reproducibly, given the evolving nature of the cyber threat. We developed a methodology and tool for identifying those areas of highest priority for mitigation by sequentially filtering out combat support functions and associated information systems of lesser concern. The methodology performs this triage both for information systems that might be attacked through cyberspace and for the combat support functions that would be affected by successful attacks. By filtering out the information systems and functions of lesser concern, this triage process identifies those information systems or functions that are both most critical for operational missions and are at the highest risk.

The Elements of the Framework

As noted in the previous section, the criticality of a combat support function to operational missions can be measured by how rapidly an operational mission would be affected by the loss of that combat support function (or information system supporting a combat support function). The overall risk of a cyber attack on an information system is defined as the product of three factors: the threat posed by an adversary, the vulnerability of the information system, and the impact to the combat support functions (excluding possible mitigations). As we discuss in the later section on impact, we exclude possible mitigations from the impact assessment. Hence, this risk is an apparent risk that is more inclusive than assessments of risk that include potential mitigations.

Figure 1.3 shows a representation of the risk and criticality to mission; the most troublesome combat support functions and information systems lie toward the upper right-hand side of the figure, indicated by the box. Preserving the combat support functions and information systems that lie within that box will reduce risk and allow operational missions to degrade most gracefully after a cyber attack. It is the functions and information systems in this box that deserve more detailed analysis, including mitigation strategies. How large this box is depends on the resources available to do this more detailed analysis.

Figure 1.3. Identifying the Highest Risk and Most Critical Information Systems and Functions



Threat

Threat is a combination of the capabilities that potential adversaries possess (both now and projected into the future) and their intent to use those capabilities to inflict harm. In this framework, threat can be expressed either by generic characteristics of unspecified adversaries or profiles of specific adversaries. It is most useful to describe threat in terms that match the relevant qualities of vulnerabilities. For example, as we describe in the next section, if one quality of vulnerability is the ability to gain access to information systems at different levels of isolation from the public, then threat is best described as whether a potential adversary has the capability and intent to access information systems at those same levels.

We note that the insider threat remains one of high concern, but is beyond the focus of this report.

Vulnerability

Generally, when analysts assess the *vulnerability* of an information system, they refer to three qualities: (1) whether the system possesses exploitable flaws, (2) whether an adversary has

knowledge of those flaws, and (3) whether an adversary has sufficient access to the system to exploit those flaws.[14] Identifying and assessing cyber vulnerabilities are two of the most challenging steps. Vulnerabilities are difficult to find, require considerable technical expertise, and come and go as new ware (software, firmware, and hardware) is introduced and existing ware is patched. For the purposes of triage, we do not need to do this technical analysis, only group together systems of comparable vulnerability and rank-order these groups.

To do this grouping and ranking, we estimate the vulnerability of a system by identifying proxies for each of these qualities that are easily assessed without the need for deep subject area expertise. Each of these three qualities of vulnerability needs to be assessed in the context of the threat vector. Two classes of threat vectors are of concern for combat support information systems—attacks through network connections such as the Internet, and attacks through the supply chain. These are not mutually exclusive because a latent implant introduced through the supply chain might be activated later via Internet connections. Given the pervasive nature of foreign involvement in the manufacture of parts and sometimes ownership of infrastructure (e.g., a SCADA system controlling power supply to a deployed location), we have considered these information systems to be approximately equally vulnerable to supply chain threats and have not defined specific proxies to distinguish supply chain vulnerabilities. Nothing in the approach precludes adding supply chain vulnerabilities in the future.

For systems of any complexity, which includes nearly all information systems, it is a fair generalization that flaws exist. Exploitable flaws can arise from deficiencies in design, implementation (including human errors), or configuration of a system.[15] The issue is whether meaningful distinctions can be made among systems with many or fewer flaws. One proxy for the relative number of flaws is how long the information system has been in operation. Because of the complexity of modern computer code and the pressures to release software rapidly, newer information systems are released with flaws that are discovered and corrected over time, leading to a tendency for older systems to have fewer flaws. Information systems that are so old that they are no longer patched would be exceptions and would tend to be more vulnerable.[16]

A simple proxy for the second quality, the degree to which an adversary is likely to have knowledge of flaws, is whether a system is commercial off-the-shelf, or was designed specifically and strictly for U.S. government use. Finally, a proxy that approximates the degree

---

[14] Often in definitions of vulnerability, the need for an adversary to have knowledge of the flaws is omitted or left implicit. We make knowledge explicit in order to align with the dimensions of threat. See DoD, 2010; Risk Steering Committee, *DHS Risk Lexicon*, 2010 Edition, Washington, D.C.: Department of Homeland Security, September 2010; and Mark Mateski, Cassandra M. Trevino, Cynthia K. Veitch, John Michalski, J. Mark Harris, Scott Maruoka, and Jason Frye, *Cyber Threat Metrics*, Albuquerque, N.M.: Sandia National Laboratories, SAND2012-2427, 2012.

[15] John D. Howard and Thomas A. Longstaff, *A Common Language for Computer Security Incidents*, Albuquerque, N.M.: Sandia National Laboratories, SAND98-8667, 1998.

[16] This generalization is most applicable to publicly available software, especially widely distributed software, where large number of users test the software and many hackers attempt to defeat security measures. For less accessible systems, the generalization is less applicable.

to which an adversary might gain access to the system to exploit the flaw is where the system resides. Is it on the World Wide Web? On the NIPRNet? Is access limited by password or public key infrastructure (PKI) certificates?[17] Does it reside on an air-gapped system? The lower the barriers to entry to the system are, the more vulnerable it is.

As a first approximation in the implementation described in the next chapter, we do not attempt to differentiate systems by the number of flaws or the adversary's likelihood of having knowledge of the flaws. Future refinements could include these additional dimensions of vulnerability.

For both threat and vulnerability, we use these proxies and assign a ranking from 1 to 5 that represents a relative degree of severity, with 5 being the most severe. The numerical values do not imply anything more than a relative ranking.

Impact

The impact wrought by a cyber attack is a cascading phenomenon. An attack on an information system affects that system, which in turn affects combat support functions or processes, which in turn affect the capability to perform operational missions (Figure 1.1). Impacts to the mission are captured on both axes in the plot in Figure 1.3. Because we estimate criticality to the operational mission by the time elapsed before the attack on combat support affects operations (represented by the *y*-axis in Figure 1.3), we limit the discussion in this section to the impact on combat support functions or processes, (one component of the *x*-axis in Figure 1.3). We assess the impact of an attack in the absence of possible mitigations. If mitigations were included here, an exhaustive analysis would have to be done of all the functions and information systems, which defeats the purpose of this exercise—to identify those functions and systems that merit such exhaustive analysis for mitigation strategies.

Again, to make this assessment easy to execute with minimal subject matter expertise, we seek proxies for impact. Two qualities of the potentially attacked information system are of interest: (1) what does the system do for combat support, and (2) what changes might take place in the information system as the result of an attack through cyberspace?

For the first question, we examined all the IT systems listed in the Component Numbered Air Force (C-NAF) Architecture (augmented by a few additional systems identified by Air Staff subject matter experts),[18] and using key words in the descriptions of those information systems, noted that the roles they perform can be generalized as

- communications support/data sharing (for situational awareness)[19]

---

[17] PKI guards use digital certificates to authenticate a user.

[18] Secretary of the Air Force, 2008.

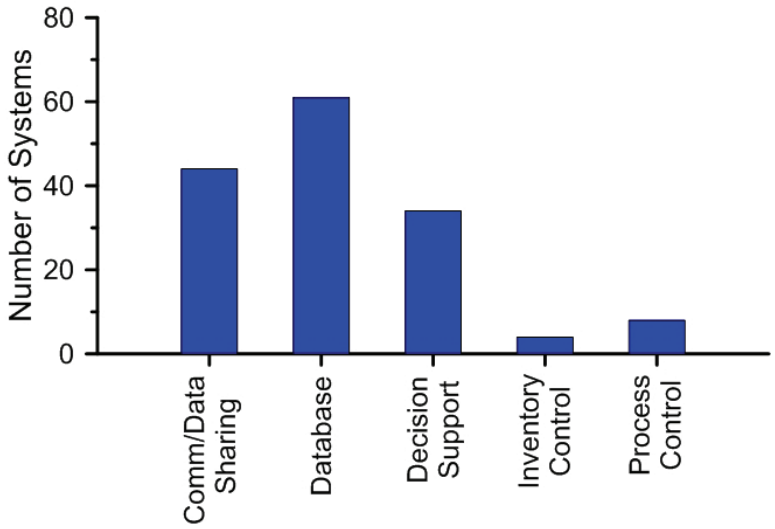
[19] Most of the systems in the communications support/data sharing category provide situational awareness to leaders. For example, systems like the Logistics, Installations, Mission Support-Enterprise View system provide an aggregated view of logistics data whose loss would not directly affect the performance of these functions. We

- database
- decision support
- inventory control
- process control.[20]

Some information systems can rightfully be assigned to more than one role, but in most cases, the dominant use is clear. Figure 1.4 shows a histogram of information systems by these categories.

The order listed above from communications support to process control gives an approximate ranking of increasing impact. In general, loss of the ability to communicate information is the least severe, and the loss of process control the most severe, although exceptions might occur in some cases.

Figure 1.4. Histogram of Combat Support Information Systems by Role



For the second question regarding the changes that might take place in an information system as the result of an attack through cyberspace, we distinguish three kinds of effects on the attacked system:

- **inability to use the system:** The Air Force simply cannot use the system, such as when a database is erased or a communications link is severed.
- **unexpected behavior:** The system is behaving erratically, under neither the control of the Air Force nor the attacker.
- **loss of control of the system:** The adversary has assumed control of the system.

---

exclude from this category purely communications systems such as the NIPRNet and phones, which are included in the category of process control.

[20] We include within the category of process control four classes of SCADA and infrastructure systems: electrical power, water, aviation fuel, and communications.

Using a process control system as an example, loss of control would indicate that the attacker now controls the process; unexpected behavior would be if the Air Force tried to change the process in some specific manner, and the response was otherwise; and inability to use the system would be the loss of ability to adjust the process.

Placing these in a ranked order of impact depends somewhat on the specific application. As a first approximation, we rank in order of increasing severity from inability to use the system to loss of control of the system. The logic is that the worst outcome would be if an adversary had full control over a system and could use it to their ends, restricted only by their knowledge of how to employ it. Consider an example of command and control. We argue that the worst case would be that the adversary took control of the system (loss of control). The next worst case would be if they attacked the system in a way in which an Air Force operator gave it a command to do one thing, and it did another (unexpected behavior). And the least worrisome case would be that the Air Force could do nothing with it (inability to use). Again, individual exceptions might occur, but consequences are bounded in the case of the inability to use a system, are wider for a system with unexpected behavior, and are most dangerous when control is surrendered to a malicious adversary.

These two dimensions of impact can be ranked simultaneously in the form of the matrix shown in Table 1.1, with a score of 5 being the most severe. Again, these numerical values have no meaning beyond a relative ranking.

Table 1.1. Categorization of Impact to Combat Support Information Systems

	Effect		
System Type	**Inability to Use**	**Unexpected Behavior**	**Loss of Control**
Communications	0.2	0.6	1.0
Database	0.4	1.2	2.0
Decision Support	0.6	1.8	3.0
Inventory Control	0.8	2.4	4.0
Process Control	1.0	3.0	5.0

Scenarios

Criticality and risk, the two dimensions of Figure 1.3, depend on the scenario of concern. Consider a scenario in which the United States is unable to achieve its objectives if impeded for a day. In that case, information systems and functions that lie within the box of interest in Figure 1.3 are much more troublesome than for a scenario in which the loss of a few weeks does not significantly change the ability to achieve national objectives. Likewise, which scenario is under consideration will determine the potential adversaries faced—and hence, threat—as well as the impact to combat support. Scenarios will also vary according to the threat posed by the adversary, including the likelihood of employing cyber attacks and the ability of an adversary to

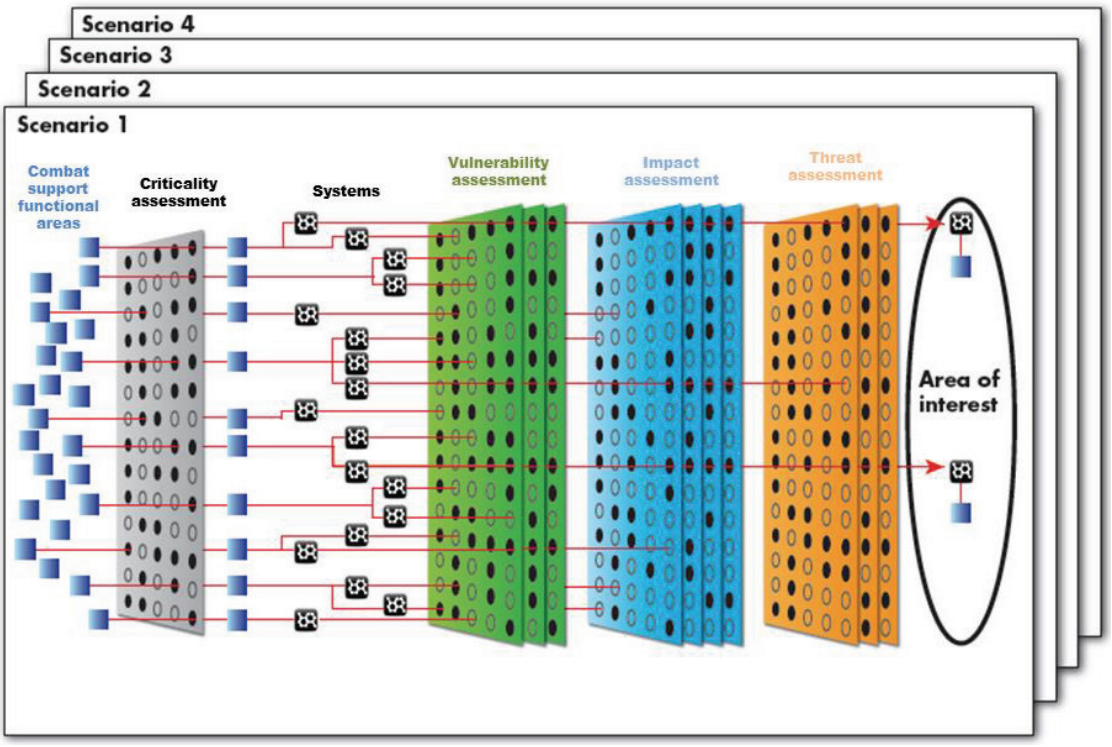
assess the success of any such attack. For any set of information systems, combat support functions, and operational missions, the assessment that generates the plot shown notionally in Figure 1.3 is scenario dependent.

Putting the Elements into a Sequential Framework

The primary motivation for our approach of identifying the functions and information systems of most concern (the box in Figure 1.3) is to avoid the need to analyze every possible system, threat, and vulnerability in developing a workable mitigation plan. The elements of the analysis identified in this chapter are: criticality to the mission, threat, vulnerability, and impact. As so many functions and information systems need to be analyzed for criticality, threat, vulnerability, and impact, the steps are ordered to minimize the amount of data and analysis needed by the user to perform the triage.

This triage can be done by ordering the assessments of the elements according to how much information and analysis needs to be done for each. Assessing the easiest first and the hardest last minimizes the work and allows more time to focus on the mitigation strategies for the most troublesome functions and information systems. The overall process is shown schematically in Figure 1.5.

Figure 1.5. A Sequential Framework for Assessing Criticality and Risk



NOTE: The methodology treats each scenario independently and does not aggregate assessments across a portfolio of scenarios.

Step 1: Select Combat Support Functional Areas

The first step is to select the domain of analysis in terms of combat support functional areas (left-most part of Figure 1.5). There are 25 functional communities identified in doctrine, but a few, such as civil engineering, are large and are worthy of dividing into subfunctions. Depending on the level of detail desired, this results in roughly 30 functional groupings.

Step 2: Determine Criticality to the Operational Mission

Moving to the right in Figure 1.5, since there are only a few dozen functional groupings to assess, the easiest first assessment is the criticality to the operational mission. This assessment of how quickly the operational mission will be affected by the loss of that functional support in terms of hours, days, weeks, months, or years can be done rapidly with minimal subject matter expertise. Functional groups with a criticality below a specified threshold can be dropped at this stage.

Step 3: Identifying Systems that Can Be Attacked Through Cyberspace

The next least labor-intensive step is to identify for each combat support function the associated information systems that can be attacked through cyberspace (IT and SCADA systems). An information system might support more than one function, and the result of this step is a list of information systems with links to combat support functions. The Air Force currently lacks a comprehensive business architecture that would supply this information. Large blocks of this information do exist, however, in the form of the C-NAF Architecture and other efforts in the Air Force—such as the Air Force Materiel Command (AFMC) Business Environment (ABE). ABE, which is an online tool that documents AFMC's the Materiel Command's business architecture in terms of policies, activities, processes, business systems, system interfaces, records, and organizations. As the Air Force better documents its business architecture, this step will be simpler and can increasingly draw data from authoritative sources.

Step 4: Vulnerability Assessment

Since hundreds of IT or SCADA systems are identified in the previous step and assessing vulnerabilities can be technically challenging, we use simple proxies for vulnerability described earlier in this chapter. These proxies can be assessed rapidly without the need for deep technical knowledge, yet capture the overall ranking of the vulnerabilities sufficiently to perform the needed triage. Systems that fall below a specified threshold can be dropped before the next step.

Step 5: Impact Assessment

The next step is to assess the impact using the categories and rankings in Table 1.1. Having identified each information system as belonging to one of five categories, this step is more manageable and can be accomplished using descriptions of information systems in the C-NAF Architecture and other similar documents.

Step 6: Threat Assessment

The final step of threat assessment is not the most demanding, but can be the most uncertain because adversaries try to keep their capabilities and intentions secret. Given the uncertainty, it is best to place it in a late stage of the triage.

Summary

The output of these six steps gives the functions and information systems that fall in the high criticality/high risk area in Figure 1.3. These functions and information systems are therefore the ones to explore more deeply for adequate mitigation strategies. It is important to leave the apertures of all the filters of the six steps wide enough so that any possible function or information system of interest comes through the triage even though some of these might have simple mitigations. It is also important to realize that an approach like this one, which depends on the use of proxies and estimates for assessing a number of attributes, carries with it a level of uncertainty in the outputs. The resulting rankings are therefore approximate and not meant to be definitive. Again, the goal in using this approach is to assist in culling the enormous task of analysis down to one that is tractable with limited resources, not as a final analysis.

The output also helps with assessing the impact of information systems to operations for compliance with National Institute of Standards and Technology guidelines.[21]

Although this methodology and tool were developed with the application of combat support in mind, the concepts are more broadly applicable. A similar assessment could be done for business support IT systems, for example, by changing the scenarios from contingencies to some desired business objective, such as completing the program objective memorandum. New information systems can be defined and functions relevant to the case at hand can be specified. The analysis framework would remain the same.

The next chapter describes a Microsoft Excel-based decision support tool that implements this methodology. It is constructed to inform combat support planning, but could be expanded to include other areas of interest.

[21] National Institute of Standards and Technology, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, Gaithersburg, Md.: U.S. Department of Commerce, NIST Special Publication 800-37, Revision 1, February 2010.

2. A Decision Support Tool for Identifying Areas of Highest Interest

This chapter describes our implementation of the methodology presented in Chapter One in the form of an easily used decision support tool. We begin with a brief overview of the tool, then describe the underlying mathematics supporting its execution.

Overview

The Logistics Cyber Risk Identification Tool (LCRIT) is a spreadsheet-hosted decision support tool created with Microsoft Excel 2007 and Visual Basic for Applications. LCRIT implements the methodology described in Chapter One. It provides a rapid analysis capability for identifying and prioritizing sources of mission risk stemming from cyber attacks against combat support information systems. We designed the tool to be usable by someone without deep cyber expertise. This requirement led to the simplifications described in Chapter One, and hence the tool's outputs should be interpreted as a first order assessment of where to best use limited resources for detailed analysis of mitigation strategies.

Since the goal of our approach is to simplify the complex problem of prioritizing cyber risk mitigation efforts, the tool breaks the problem down into a limited number of tractable questions that do not require deep subject matter expertise. The model is prepopulated with a list of combat support functions and subfunctions and many of the associated systems. For these, the requisite information needed is already entered into the model, requiring the user to only answer questions about any extra functions, information systems, contingencies, or adversaries the user wishes to add. These data represent our best estimate of the situation as of 2013; the user can change these as needed. Using this information, the tool performs a series of calculations and outputs the results in an easily understood format, that of Figure 1.3, identifying the functions and information systems that present the greatest cyber mission risk and therefore warrant further attention for developing appropriate mitigation strategies.

Implementation

In this section, we briefly review each of the elements of the tool. Most of the values of these elements are user adjustable. We highlight those elements provided as default values that can be used for most tool runs, and those that must be altered by the user for each run.

Scenarios

Each tool run analyzes a specific scenario. For the purposes of this tool, a scenario consists of a contingency *m*, which provides the baseline against which criticality of the function or information system is assessed, and an adversary *a*, which specifies the threat of attack through cyberspace. (Table 2.1 summarizes all mathematical notation.) While the tool can store data for multiple scenarios, each individual run analyzes a specific scenario and the results produced by each run are only applicable to that selected scenario.

Table 2.1. Summary of Mathematical Notation

Symbol	Meaning	Constraints
a	Adversary	None
A_{da}	Degree to which adversary *a* can access domain *d*	$A_{da} \in \{0.0, 0.5, 1.0\}$
C_{mf}	Relative time-criticality of function *f* to contingency *m*	$C_{mf} \in \{0, 1, 2, 3, 4, 5\}$
C_s	Maximum relative time-criticality of all functions supported by system *s*	None
d	Domain	None
D_{fs}	Indicates whether function *f* depends on system *s*	$D_{fs} \in \{0, 1\}$
e	Effect	None
E_{ea}	Degree to which adversary *a* is capable of achieving effect *e*	$E_{ea} \in \{0.0, 0.5, 1.0\}$
f	Function or subfunction	None
H_{sd}	Indicates whether system *s* is hosted in domain *d*	$H_{sd} \in \{0, 1\}$
I_{re}	Relative impact to contingency of effect *e* on system with role *r*	None
m	Contingency	None
r	Role of each information system *s*	None
R_{sr}	Indicates whether system *s* has role *r*	$R_{sr} \in \{0, 1\}$
s	System	None
V_{sa}	Relative vulnerability of system *s* to adversary *a*	None
ρ_{af}	Relative risk to function *f* posed by an attack by adversary *a*	None
ρ_{as}	Relative risk to information system *s* posed by an attack by adversary *a*	None

Contingencies

The tool considers contingencies only for the purposes of determining the time criticality of a combat support function or subfunction. Hence, the only data for a particular contingency are those that define the relationship between each contingency and each supporting function. These relationships are discussed below.

We have prepopulated the tool with a default major combat operation contingency. The user can insert additional contingencies in the tool.

Functions

In the tool, functions represent the combat support functions and subfunctions discussed in Chapter One. Our list of functions is derived from combat support doctrine and should be suitable for most tool uses in the combat support community.[22] We have assessed the criticality of each function to a particular contingency. For any user-added function or contingency, the user must assess the time criticality of each function to any new contingency (how quickly the loss of the function would affect the operational mission—hours, days, weeks, months, or years). These data populate a matrix with elements C_{mf} that give the relative time criticality of function f to contingency m.

Information Systems

Information systems are the IT and SCADA systems on which the Air Force depends to perform combat support functions and that can potentially be attacked through cyberspace. The tool is populated with a number of information systems used by combat support, most of which are extracted from the C-NAF Architecture. For each of these, we have determined which functions depend on which information systems. A matrix with elements D_{fs} has a value of 1 if a function f depends on a system s, and 0 otherwise. For the purposes of vulnerability and threat assessment, each information system is specified to reside on a domain d (the domains are: World-Wide, PKI-protected, password-protected, or air-gapped system). A matrix is defined with elements H_{sd} that take a value of 1 if the system s resides on domain d, and 0 otherwise. Finally, each information system is assigned a role r (communications support/data sharing, database, decision support, inventory control, or process control). A matrix is defined with elements R_{sr} that take a value of 1 if system s has role r, and 0 otherwise.

The user only needs to add values to these matrices for any functions or information systems that the user adds.

Adversaries

Each run of the tool analyzes a specific scenario contingency m combined with a specific adversary a. Adversaries are defined by their capability to access each domain d and impart some effect e on systems hosted in those domains. The effects are those described in Chapter One: inability to use the system, unexpected behavior, and loss of control of the system. The relative degree to which an adversary a can access domain d is given by elements of a matrix A_{da}, which takes on values of 0, 0.5, or 1. The value 0 indicates no access; a value of 0.5 indicates occasional access, and a value of 1 indicates persistent access. A matrix with elements E_{ea} specifies the degree to which adversary a can achieve an effect e.[23] Values for E_{ea} are either 0 or

[22] U.S. Air Force, 2013.

[23] Currently, this parameter is not system dependent. It could be expanded in the future to be the degree to which adversary a can achieve an effect e on system s.

1. A value of 0 indicates the adversary has not demonstrated the ability to achieve the effect. A value of 1 indicates that the adversary has demonstrated the ability to achieve the effect.

The user can add values for any adversaries added to the tool.

We note that cyber attacks can come via numerous vectors, including through the supply chain by embedding malicious hardware, firmware, or software in supply parts. We do not include supply-chain threats in the tool, but it could be expanded to include such threats in the form of adversary capabilities. However, new proxies for vulnerability would need to be developed to fully cover this threat vector.

Calculations

The tool's primary outputs are the function and system plots described in Chapter One and shown schematically in Figure 1.3. The tool generates two plots in this form: one for functions and one for information systems. The calculations that determine the location of each function or information system in the plot are given here.

Information Systems

For each information system *s*, the position on the abscissa is given by the risk from a threat from adversary *a*:

$$\rho_{as} = V_{sa} \max_{e} \left[\max_{r} (E_{ea} I_{re} R_{sr}) \right],$$

where I_{re} is Table 1.1 and the vulnerability of system *s* to a cyber attack by adversary *a* is given by:

$$V_{sa} = \max_{d} (A_{da} H_{sd}).$$

The position on the ordinate is given by the criticality of the information system:

$$C_s = \max_{f} (D_{fs} C_{mf}).$$

Functions

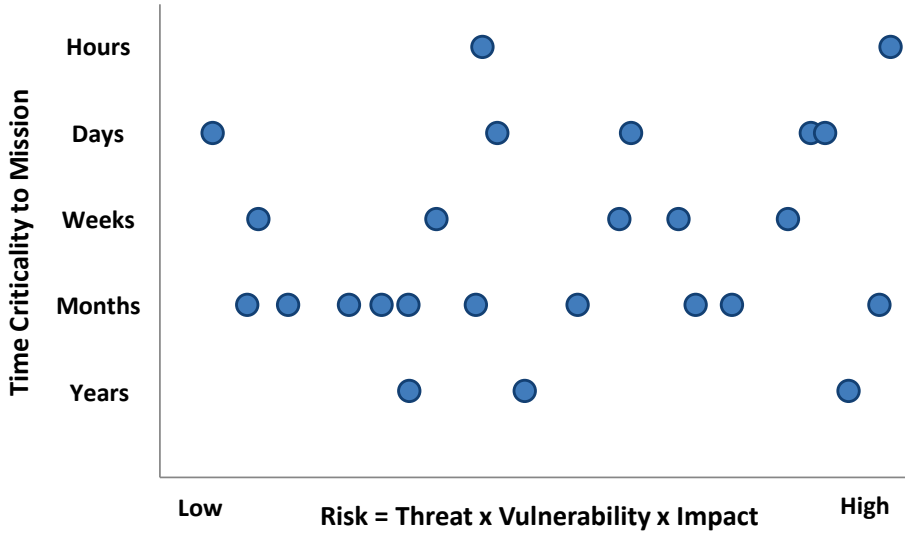
For each function *f*, the position on the abscissa is given by the risk from a threat from adversary *a*:

$$\rho_{af} = \sum_{s} D_{fs} \rho_{as}$$

and the position on the ordinate is given by C_{mf}.

For both information systems and functions, the tool produces plots in the form of the notional example in Figure 2.1. The user can examine each point on the plot to determine which function or system is represented. The tool executes all calculations within less than one second.

Figure 2.1. Notional Output: Combat Support Function Risk and Mission Time Criticality



Conclusions

In the event of a cyber attack, identifying the most troublesome combat support functions and information systems for operational mission continuity appears overwhelming. There are dozens of functions and hundreds of information systems. The threats and vulnerabilities continuously evolve and can require technical knowledge to understand in full. On top of this, the cascading events—from an adversary's actions, to the effect on information systems, to the impact to combat support functions, and finally to the impact to the operational mission—can be difficult to trace.

Our premise is that mitigation strategies should focus on operational mission assurance rather than the more restricted information assurance. That is, the goal should be the continuity of the operational mission, not just the continuity of the operation of the information systems that support it. The methodology and decision support tool to implement that methodology presented in this report makes this problem more tractable by identifying the functions and information systems most critical to the operational mission and most at risk in the cyber domain. This first-order triage can be done rapidly without deep cyber expertise. The ranking of the functions and information systems is an estimate to guide where to apply limited resources for more detailed analysis of mitigation. The simplicity allows the triage to be done as frequently as needed to assess risks and identify mitigations as threats and vulnerabilities continuously evolve.

We stress that the methodology developed in this report and implemented in the associated LCRIT give approximate rankings that should not be treated as definitive. The results place the most critical functions and information systems toward the top of the rankings and the least toward the bottom, but given the use of proxies for the assessments, there will be some

inaccuracies in detail. We recommend that the results be used as triage to determine a range of functions and information systems for further scrutiny. How many to examine in more detail will depend on the resources available, which determines the size of the box in Figure 1.3; the more limited the resources, the smaller the box and the higher the value of doing triage, but the greater the risk of missing a function or information system of concern.

This triage methodology and decision support tool provide the first step in ensuring that operations can endure during and after cyber attacks on combat support information systems.

References

Albright, David, Paul Brannan, and Christina Walrond, *Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?* Washington, D.C.: Institute for Science and International Security, December 22, 2010. As of December 29, 2013: http://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/

Allenby, Brad, and Jonathan Fink, "Toward Inherently Secure and Resilient Societies," *Science*, Vol. 309, 2005.

Clarke, Richard A., and Robert Knake, *Cyber War: The Next Threat to National Security and What to Do About It*, New York: HarperCollins, 2010.

Committee on National Security Systems, *National Information Assurance (IA) Glossary*, Washington, D.C., CNSS Instruction No. 4009, April 26, 2010. As of December 29, 2013: http://www.ncix.gov/publications/policy/docs/CNSSI_4009.pdf

Falliere, Nicolas, Liam O. Murchu, and Eric Chien, *W32.Stuxnet Dossier*, Version 1.4, Symantec Security Response, February 2011. As of December 29, 2013: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

Freedman, Lawrence, *Strategy: A History*, New York: Oxford University Press, 2013.

Howard, John D., and Thomas A. Longstaff, *A Common Language for Computer Security Incidents*, Albuquerque, N.M.: Sandia National Laboratories, SAND98-8667, October 1998.

Libicki, Martin C., *Cyberdeterrence and Cyberwar*, Santa Monica, Calif.: RAND Corporation, MG-877-AF, 2009. As of December 29, 2013: http://www.rand.org/pubs/monographs/MG877.html

Mateski, Mark, Cassandra M. Trevino, Cynthia K. Veitch, John Michalski, J. Mark Harris, Scott Maruoka, and Jason Frye, *Cyber Threat Metrics*, Albuquerque, N.M.: Sandia National Laboratories, SAND2012-2427, 2012.

Musman, Scott, Aaron Temin, Mike Tanner, Richard Fox, and Brian Pridemore, "Evaluating the Impact of Cyber Attacks on Missions," *M&S Journal*, Vol. 8, No. 2, Summer 2013, pp. 25–35.

National Institute of Standards and Technology, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, Gaithersburg,

Md.: U.S. Department of Commerce, NIST Special Publication 800-37, Revision 1, February 2010. As of December 29, 2013: http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf

Risk Steering Committee, *DHS Risk Lexicon*, 2010 Edition, Washington, D.C.: Department of Homeland Security, September 2010. As of December 29, 2013: http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf

Secretary of the Air Force, Warfighting Integration and Chief Information Office, "Component NAF 2008 Architecture: Federated AFFOR/AOC Architecture," Version 2.1, January 14, 2008, distribution authorized to DoD and U.S. defense contractors only.

U.S. Air Force, *Cyberspace Operations*, Washington, D.C.: Department of the Air Force, Air Force Policy Directive 10-17, July 31, 2012.

———, *Combat Support*, Washington, D.C.: United States Air Force, Air Force Doctrine Document 4-0, April 23, 2013. As of December 29, 2013: http://static.e-publishing.af.mil/production/1/af_cv/publication/afdd4-0/afdd4-0.pdf

U.S. Department of Defense, *Cybersecurity*, Instruction 8500.01, Washington, D.C.: DoD Chief Information Officer, 14 March 2014.

———, *Department of Defense Dictionary of Military and Associated Terms*, Washington, D.C.: Joint Chiefs of Staff, Joint Publication 1-02, November 8, 2010 (as amended through November 15, 2013). As of December 29, 2013: http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf

Verizon RISK Team, *2013 Data Breach Investigations Report*, Verizon, 2013. As of December 29, 2013: http://www.verizonenterprise.com/DBIR/2013/

PROJECT AIR FORCE

www.rand.org

$16.95

ISBN-10 0-8330-8629-4
ISBN-13 978-0-8330-8629-7

RR-620-AF